Contents

CONTEXT SR0_Path

SETS

PATH

ROUTE

CONSTANTS

PathConflict

Route2InitPath

PathSub

NullPath

AXIOMS

assocMult_Path_conflic: $PathConflict \in PATH \leftrightarrow PATH$

axm1: $\forall p \cdot p \in PATH \Rightarrow (PathConflict \cap id = \varnothing)$

axm2: $\forall p \cdot p \in PATH \Rightarrow (PathConflict = PathConflict^{-1})$

axm3: $\forall p \cdot p \in PATH \Rightarrow (finite(PATH))$

assocRoute2Path: $Route2InitPath \in ROUTE \rightarrow PATH$

assocPath_SubPath: $PathSub \in PATH \leftrightarrow PATH$

axm4: $\forall p \cdot p \in PATH \Rightarrow (\forall p1, p2 \cdot p1 \in PathSub[\{p2\}] \land p \notin PathConflict[\{p2\}] \Rightarrow p \notin PathConflict[\{p1\}])$

axm5: $\forall p \cdot p \in PATH \Rightarrow NullPath \in PathSub[\{p\}]$

axm6: $NullPath \in PATH$

END

CONTEXT SR1_Block
EXTENDS SR0_Path
SETS
BLOCK
CONSTANTS
Path2Block
PathReduce
AXIOMS
axm1: $Path2Block \in PATH \leftrightarrow BLOCK$
axm2: $\forall p \cdot p \in PATH \Rightarrow (\forall q \cdot q \notin PathConflict[\{p\}] \Leftrightarrow (Path2Block[\{p\}] \cap Path2Block[\{q\}] = \varnothing))$
axm3: $PathReduce \in \{PATH \setminus \{NullPath\}\} \rightarrow (BLOCK \rightarrow PATH)$
axm4: $\forall p \cdot p \in PATH \setminus \{NullPath\} \Rightarrow (\exists b \cdot b \in BLOCK \Rightarrow PathReduce(\{p\})(b) \in PathSub[\{p\}])$
axm5: $\forall p \cdot p \in PATH \setminus \{NullPath\} \Rightarrow (\exists b \cdot b \in BLOCK \Rightarrow Path2Block[\{PathReduce(\{p\})(b)\}] = Path2Block[\{p\}] \setminus \{b\})$
axm6: $Path2Block[\{NullPath\}] = \varnothing$
END

CONTEXT SR2_Point
EXTENDS SR1_Block
SETS
POS
CONSTANTS
POINT
Default_Point2Pos
Route_Point2Pos
AXIOMS
axm1: $POINT \subseteq BLOCK$
axm2: $Route\_Point2Pos \in Route \rightarrow (POINT \rightarrow POS)$
axm4: $Default\_Point2Pos \in POINT \rightarrow POS$
axm3: $\forall pos \cdot pos \in POS \Rightarrow (finite(POS))$
END

CONTEXT SR3_TVD
EXTENDS SR2_Point
SETS
STATUS
CONSTANTS
Vacant
Occupied
AXIOMS
axm1: $partition(STATUS, \{Vacant\}, \{Occupied\})$
END

CONTEXT SR4_Signal
EXTENDS SR3_TVD
SETS
ASPECT
CONSTANTS
Go
Stop
AXIOMS
axm1: $partition(ASPECT, \{Go\}, \{Stop\})$
END

MACHINE SR_M0
SEES SR0_Path
VARIABLES

Route_Req
Route_Cel
Route_Occ
Route2Path

INVARIANTS

typeof_Route_Res: $Route\_Req \subseteq ROUTE$
typeof_Route_Cel: $Route\_Cel \subseteq ROUTE$
typeof_Route_Occ: $Route\_Occ \subseteq ROUTE$
safety_Req: $\forall r1, r2 \cdot (r1 \neq r2 \wedge r1 \in Route\_Occ \wedge r2 \in Route\_Occ) \Rightarrow (PathConflict^{-1}[Route2Path[\{r1\}]] \cap Route2Path[\{r2\}] = \varnothing)$
typeof_CurrRoute2Path: ⟨theorem⟩ $Route2Path \in ROUTE \nrightarrow PATH$
inv1: $\forall r \cdot r \in Route\_Occ \Rightarrow (Route2Path[\{r\}] \neq \varnothing)$

EVENTS
Initialisation
begin
act1: $Route\_Req := \varnothing$
act5: $Route\_Cel := \varnothing$
act2: $Route\_Occ := \varnothing$
act3: $Route2Path := \varnothing$
end
Event Route_Reserve ⟨ordinary⟩ $\widehat{=}$
any
r
where
grd1: $r \in Route\_Req$
grd2: $r \notin Route\_Cel$
grd3: $r \notin dom(Route2Path)$
grd4: $PathConflict[Route2InitPath[\{r\}]] \cap ran(Route2Path) = \varnothing$
then
act1: $Route2Path := Route2Path \cup \{r \mapsto Route2InitPath(r)\}$
act2: $Route\_Req := Route\_Req \setminus \{r\}$
end
Event Route_Release2 ⟨ordinary⟩ $\widehat{=}$
any
r
where
grd1: $r \in dom(Route2Path)$
grd2: ⟨theorem⟩ $Route2Path(r) = NullPath$
grd3: $r \notin Route\_Occ$
then
act1: $Route2Path := \{r\} \lhd Route2Path$
end
Event Route_Release1 ⟨ordinary⟩ $\widehat{=}$
any
r
where
grd1: $r \in Route\_Req \cup dom(Route2Path)$
grd2: $r \in Route\_Cel$
grd3: $r \notin Route\_Occ$
then
act1: $Route\_Req := Route\_Req \setminus \{r\}$
act2: $Route\_Cel := Route\_Cel \setminus \{r\}$
act3: $Route2Path := \{r\} \lhd Route2Path$

end

Event Train_Enter ⟨ordinary⟩ $\widehat{=}$

any

r

where

grd1: $r \in dom(Route2Path)$

grd2: $r \notin Route\_Occ$

then

act1: $Route\_Occ := Route\_Occ \cup \{r\}$

end

Event Train_Leave ⟨ordinary⟩ $\widehat{=}$

any

r

where

grd1: $r \in Route\_Occ$

grd2: $r \in dom(Route2Path)$

then

act1: $Route\_Req := Route\_Req \setminus \{r\}$

act3: $Route\_Occ := Route\_Occ \setminus \{r\}$

act2: $Route2Path(r) := NullPath$

end

Event Route_Request ⟨ordinary⟩ $\widehat{=}$

any

r

where

grd1: $r \in ROUTE$

then

act1: $Route\_Req := Route\_Req \cup \{r\}$

end

Event Route_Cancel ⟨ordinary⟩ $\widehat{=}$

any

r

where

grd1: ⟨theorem⟩ $r \in Route\_Req \cup dom(Route2Path)$

then

act1: $Route\_Cel := Route\_Cel \cup \{r\}$

end

END

MACHINE SR_M1
REFINES SR_M0
SEES SR1_Block
VARIABLES
Route_Req
Route_Cel
Route_Occ
Route2Path
Block2Route
INVARIANTS
inv1: $Block2Route \in BLOCK \pfun ROUTE$
inv2: $\forall p \cdot p \in PATH \Rightarrow (\forall q \cdot q \notin PathConflict[\{p\}] \Leftrightarrow (Path2Block[\{p\}] \cap Path2Block[\{q\}] = \varnothing))$
EVENTS
Initialisation ⟨extended⟩
begin
act1: $Route\_Req := \varnothing$
act5: $Route\_Cel := \varnothing$
act2: $Route\_Occ := \varnothing$
act3: $Route2Path := \varnothing$
act4: $Block2Route := \varnothing$
end
Event Block_Reserve ⟨ordinary⟩ $\widehat{=}$
any
r
p
where
grd1: $r \in Route\_Req$
grd3: $r \notin Route\_Cel$
grd6: $r \notin Route\_Occ$
grd5: $p \in PATH$
grd4: $p = Route2InitPath(r)$
grd2: $Path2Block[\{p\}] \cap dom(Block2Route) = \varnothing$
then
act1: $Block2Route := Block2Route \cup \{Path2Block(p) \mapsto r\}$
end
Event Block_Release2 ⟨ordinary⟩ $\widehat{=}$
any
r
cp
sp
b
where
grd1: $r \in Route\_Occ$
grd2: $r \in dom(Route2Path)$
grd3: $cp = Route2Path(r)$
grd4: $cp \neq NullPath$
grd6: $b \in Path2Block[\{cp\}]$
grd5: $sp = PathReduce(\{cp\})(b)$
then
act1: $Block2Route := \{b\} \domsub Block2Route$
act2: $Route2Path(r) := sp$
end
Event Block_Release1 ⟨ordinary⟩ $\widehat{=}$
any
r
where
grd1: $r \in Route\_Cel$

grd2: $r \in dom(Route2Path)$
grd3: ⟨theorem⟩ $r \notin Route\_Occ$

then

act1: $Block2Route := Block2Route \rhd \{r\}$
act2: $Route2Path(r) := NullPath$

end

Event Route_Request ⟨ordinary⟩ $\widehat{=}$
extends Route_Request

any

r

where

grd1: $r \in ROUTE$

then

act1: $Route\_Req := Route\_Req \cup \{r\}$

end

Event Route_Cancel ⟨ordinary⟩ $\widehat{=}$
extends Route_Cancel

any

r

where

grd1: ⟨theorem⟩ $r \in Route\_Req \cup dom(Route2Path)$

then

act1: $Route\_Cel := Route\_Cel \cup \{r\}$

end

Event Route_Reserve ⟨ordinary⟩ $\widehat{=}$
extends Route_Reserve

any

r

where

grd1: $r \in Route\_Req$
grd2: $r \notin Route\_Cel$
grd3: $r \notin dom(Route2Path)$
grd4: $PathConflict[Route2InitPath[\{r\}]] \cap ran(Route2Path) = \varnothing$
grd5: $Block2Route^{-1}(r) = Path2Block(Route2InitPath(r))$

then

act1: $Route2Path := Route2Path \cup \{r \mapsto Route2InitPath(r)\}$
act2: $Route\_Req := Route\_Req \setminus \{r\}$

end

Event Route_Release1 ⟨ordinary⟩ $\widehat{=}$
extends Route_Release1

any

r

where

grd1: $r \in Route\_Req \cup dom(Route2Path)$
grd2: $r \in Route\_Cel$
grd3: $r \notin Route\_Occ$

then

act1: $Route\_Req := Route\_Req \setminus \{r\}$
act2: $Route\_Cel := Route\_Cel \setminus \{r\}$
act3: $Route2Path := \{r\} \lhd Route2Path$

end

Event Route_Release2 ⟨ordinary⟩ $\widehat{=}$
extends Route_Release2

any

r

where

grd1: $r \in dom(Route2Path)$
grd2: ⟨theorem⟩ $Route2Path(r) = NullPath$

grd3: $r \notin Route\_Occ$

then

act1: $Route2Path := \{r\} \lhd Route2Path$

end

Event Train_Enter ⟨ordinary⟩ $\widehat{=}$

extends Train_Enter

any

r

where

grd1: $r \in dom(Route2Path)$

grd2: $r \notin Route\_Occ$

then

act1: $Route\_Occ := Route\_Occ \cup \{r\}$

end

Event Train_Leave ⟨ordinary⟩ $\widehat{=}$

extends Train_Leave

any

r

where

grd1: $r \in Route\_Occ$

grd2: $r \in dom(Route2Path)$

grd3: $Block2Route^{-1}[\{r\}] = \varnothing$

then

act1: $Route\_Req := Route\_Req \setminus \{r\}$

act3: $Route\_Occ := Route\_Occ \setminus \{r\}$

act2: $Route2Path(r) := NullPath$

end

END